ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

(Laboratorio di)
Amministrazione di sistemi

Linux Networking

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

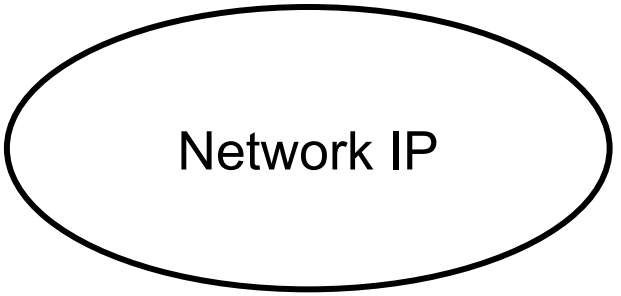
Acknowledgements

- Tutte le slide su richiami di reti locali, vlan, reti IP, routing sono basate su materiali di
  - Franco Callegati <franco.callegati@unibo.it>
  - Walter Cerroni <walter.cerroni@unibo.it>

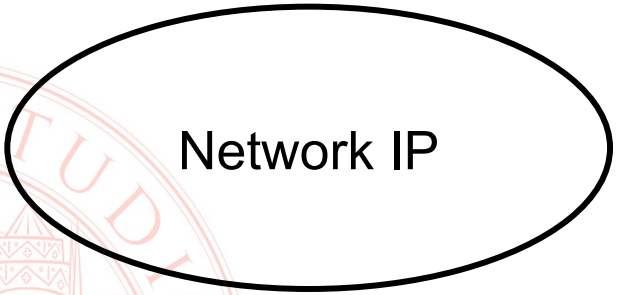
Come funziona Internet

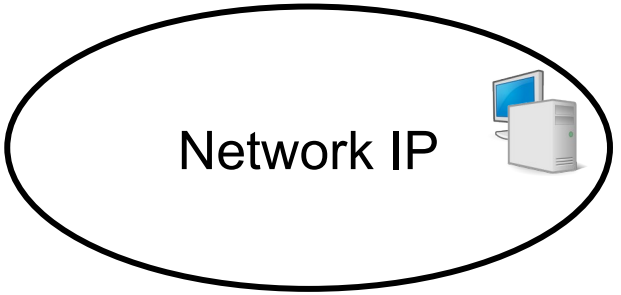
- Internet è una grande “rete di reti”
- La componente elementare è la network IP
  - Ogni network IP è una sorta di isola
    - L’isola tipicamente contiene calcolatori che fungono da nodi terminali della rete detti host
  - Le isole sono interconnesse da apparati che svolgono la funzione di “ponte”
    - Si tratta di calcolatori specializzati detti router o gateway

Internet: reti di reti



Tante Network IP isolate





Indirizzo globale e indirizzo locale

- Indirizzo globale
  - È valido per tutta la rete
  - Deve essere univoco (non devono esistere indirizzi replicati) per evitare ambiguità
  - Va "assegnato" seguendo una procedura di gestione "globale" che assicura la non replicazione
- Indirizzo locale
  - È valido limitatamente ad un certa sottoporzione della rete
    - Internamente ad un terminale
    - In un dominio di rete specifico
  - Può non essere globalmente univoco
  - Può essere assegnato con una procedura puramente "locale"

Rete logica e rete fisica

- Nella terminologia di Internet si definisce
  - **Rete logica**: la network IP (o **subnet**) a cui un Host appartiene logicamente
  - **Rete fisica**: la rete (tipicamente **LAN**) a cui un Host è effettivamente connesso
- La rete fisica normalmente ha capacità di instradamento e può avere indirizzi locali (es. indirizzi MAC)
- L'architettura a strati nasconde gli indirizzi fisici e consente alle applicazioni di lavorare solo con indirizzi IP

La network IP

- I calcolatori di una network IP sono connessi dalla medesima infrastruttura di rete fisica (livelli 1 e 2)

- Ipotesi fondamentale
  - Tutti gli host appartenenti alla medesima network IP sono in grado di parlare tra loro grazie alla tecnologia con cui essa viene implementata

Indirizzi IP

- **Associazione univoca indirizzo -> sistema (*host*)**
  - **(non è imposto il contrario -> *multi-homed host*)**
- **Indirizzi IPv4: 32 bit divisi in 4 byte, normalmente rappresentati con 4 numeri in base 10 separati da punti (*dotted decimal notation*)**
  - **Esempio: 137.204.59.1**
- **Ogni indirizzo fa parte di una rete *(subnet)* che inizia da un indirizzo di *network***
- **In origine l' estensione era implicita, ora è specificata da una *netmask***
  - **Una subnet logica coincide con una LAN fisica**
  - **Per instradare un pacchetto verso la destinazione non serve considerare il suo indirizzo, basta la subnet cui appartiene**

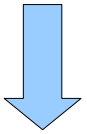
Reti class-based

Originariamente sono state definite *classi* di indirizzi, ovvero raggruppamenti da usare per i sistemi di una rete locale, in cui i byte erano rigidamente divisi tra network id e host id:

- **128 reti di Classe A (contenenti fino a 16 milioni di host circa):**
  - **indirizzi da 0.*.*.* a 127.*.*.***
- **16.384 reti di Classe B (contenenti fino a 65000 host circa):**
  - **indirizzi da 128.0.*.* a 191.255.*.***
- **2.097.152 reti di Classe C (contenenti fino a 254 host):**
  - **indirizzi da 192.0.0.* a 223.255.255.***
- **Gli indirizzi da 224.*.*.* a 239.*.*.* sono riservati al *multicast***
- **Gli indirizzi da 240.*.*.* a 255.*.*.* sono riservati a usi futuri**

Il vantaggio sulle LAN

- Host su una stessa rete locale:
  - collocati in una stessa area, servita da un determinato apparato di rete
  - numericamente identificati da indirizzi di una stessa subnet



- Per raggiungerli non ho bisogno di sapere dove si trova ognuno, mi basta sapere come raggiungere la subnet

CIDR

- Poche classi di dimensioni fissate = spreco di indirizzi
- Soluzione: CIDR (*classless inter-domain routing*)
- Con classless-IP gli indirizzi sono visti come una stringa di 32 bit divisa in net-id e host-id in un punto arbitrario, anzichè per byte.
  - Unico vincolo (ovvio): la dimensione di una rete è potenza di 2 (in questo esempio 2^6 = 64 indirizzi)

    144 . 156 . 166 . 151

    1 0 0 1 0 0 0 0 1 0 0 1 1 1 0 0 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 1

    26 bit net-id 6 bit host-id
- Una rete locale è identificata per mezzo di un *network address* e di una *netmask*, noti a tutti gli host che ne fanno parte.

Netmask, network, broadcast

- Serve un modo per specificare dove cade la divisione
- La *netmask* è un valore di 32 bit composto da
  - tanti “1” quanti sono i bit che identificano la subnet, seguiti da
  - tanti “0” quanti sono i bit che specificano l'host al suo interno
  - Nell'esempio precedente:
    11111111.11111111.11111111.11000000 = 255.255.255.192
- Due valori in ogni subnet hanno un significato speciale e non possono essere usati per indirizzare un host:
  - Network address (ottenuto mettendo a 0 tutti i bit dell’host-id)
    - 10010000.10011100.10100110.10000000 = 144.156.166.128
  - Broadcast (ottenuto mettendo a 1 tutti i bit dell’host-id)
    - 10010000.10011100.10100110.10111111 = 144.156.166.191

Doppio indirizzamento nella LAN/subnet!

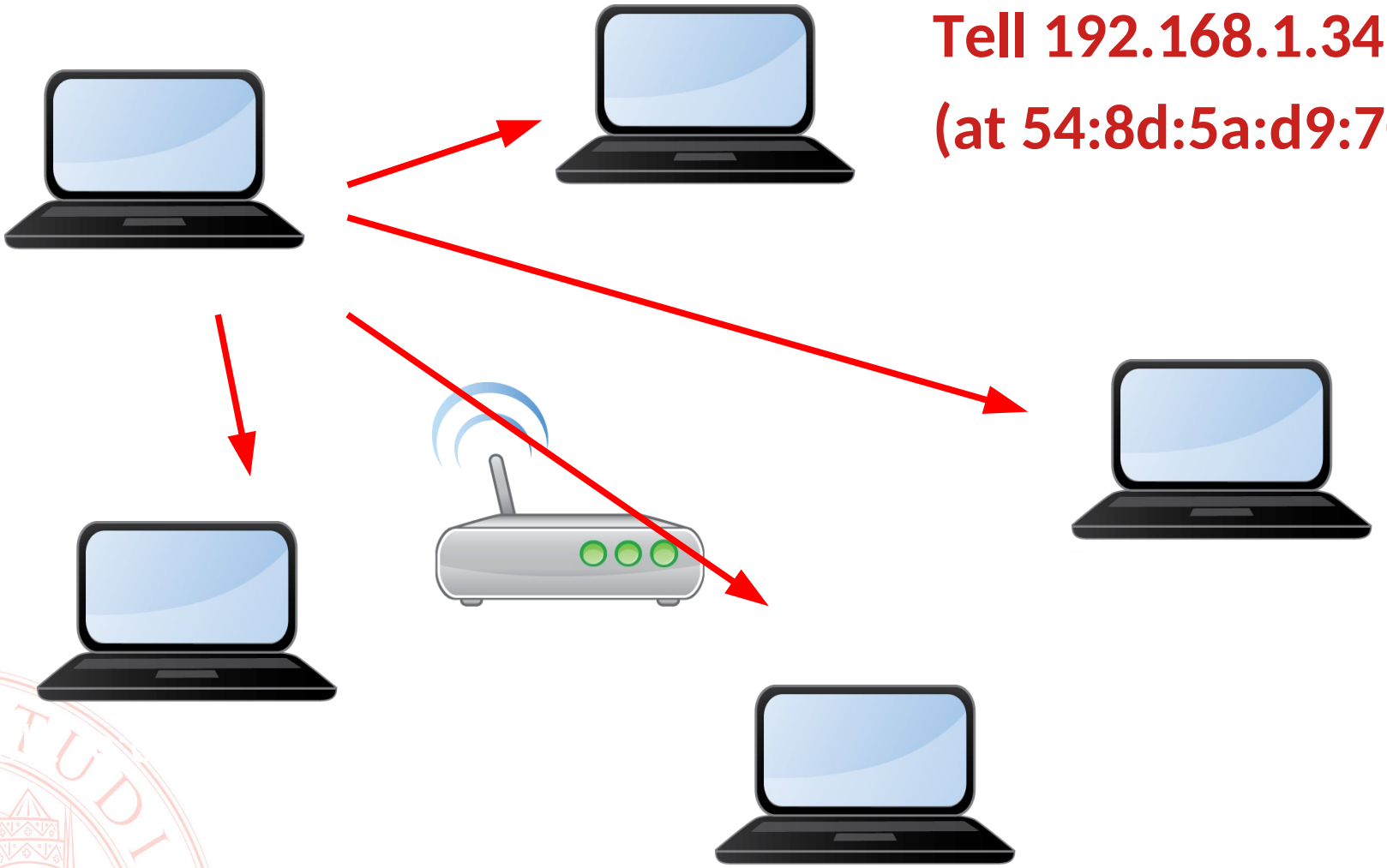
- Ogni dispositivo della LAN ha un MAC address
  - L'inoltro fisico del traffico avviene tra le schede di rete
- Ma è anche un dispositivo della rete IP con un indirizzo
  - Le applicazioni si "conoscono" come endpoint IP
- Come tradurre un indirizzo nell'altro?
- Address Resolution Protocol (ARP – RFC 826)

ARP request - broadcast

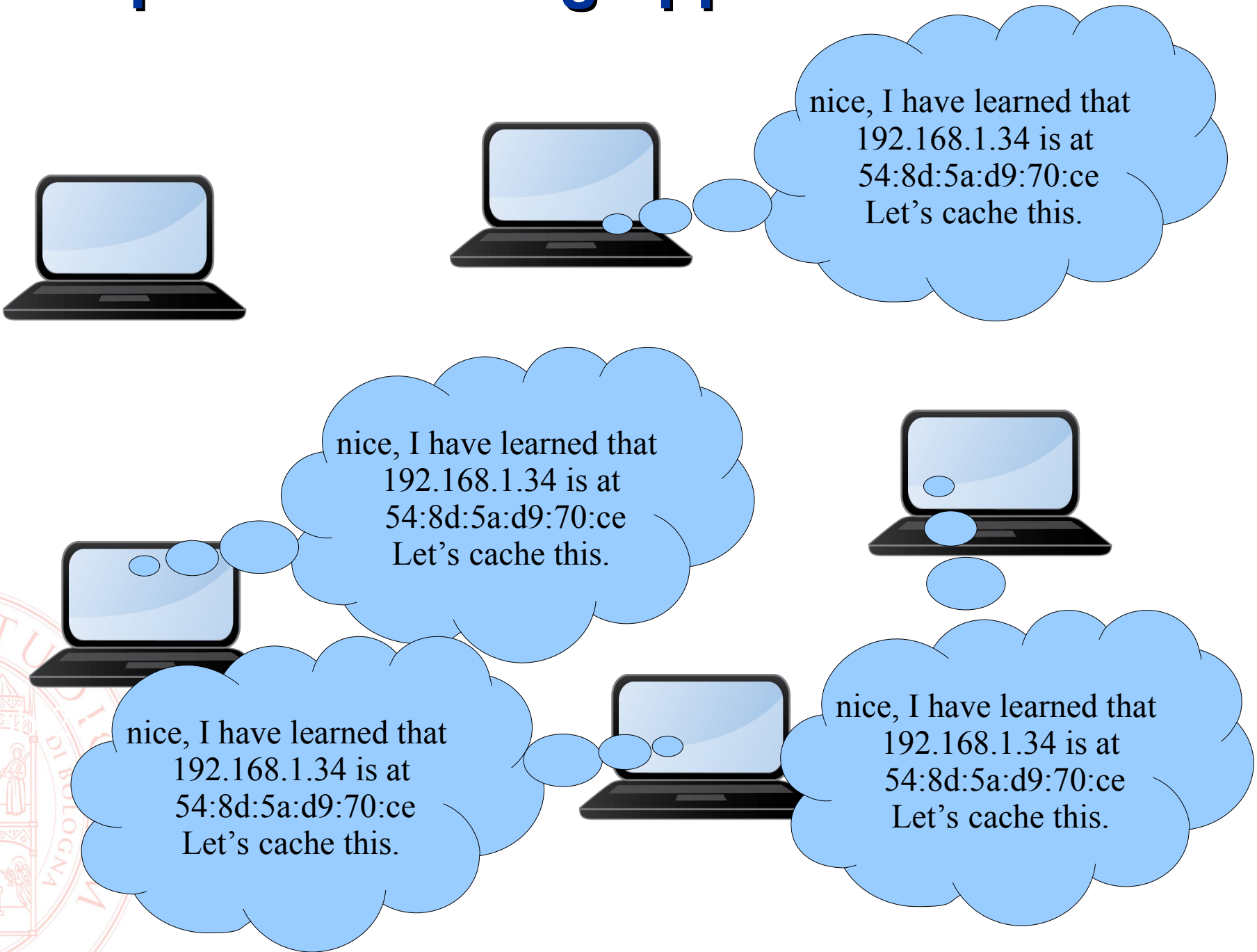
Who has 192.168.1.76?

Tell 192.168.1.34

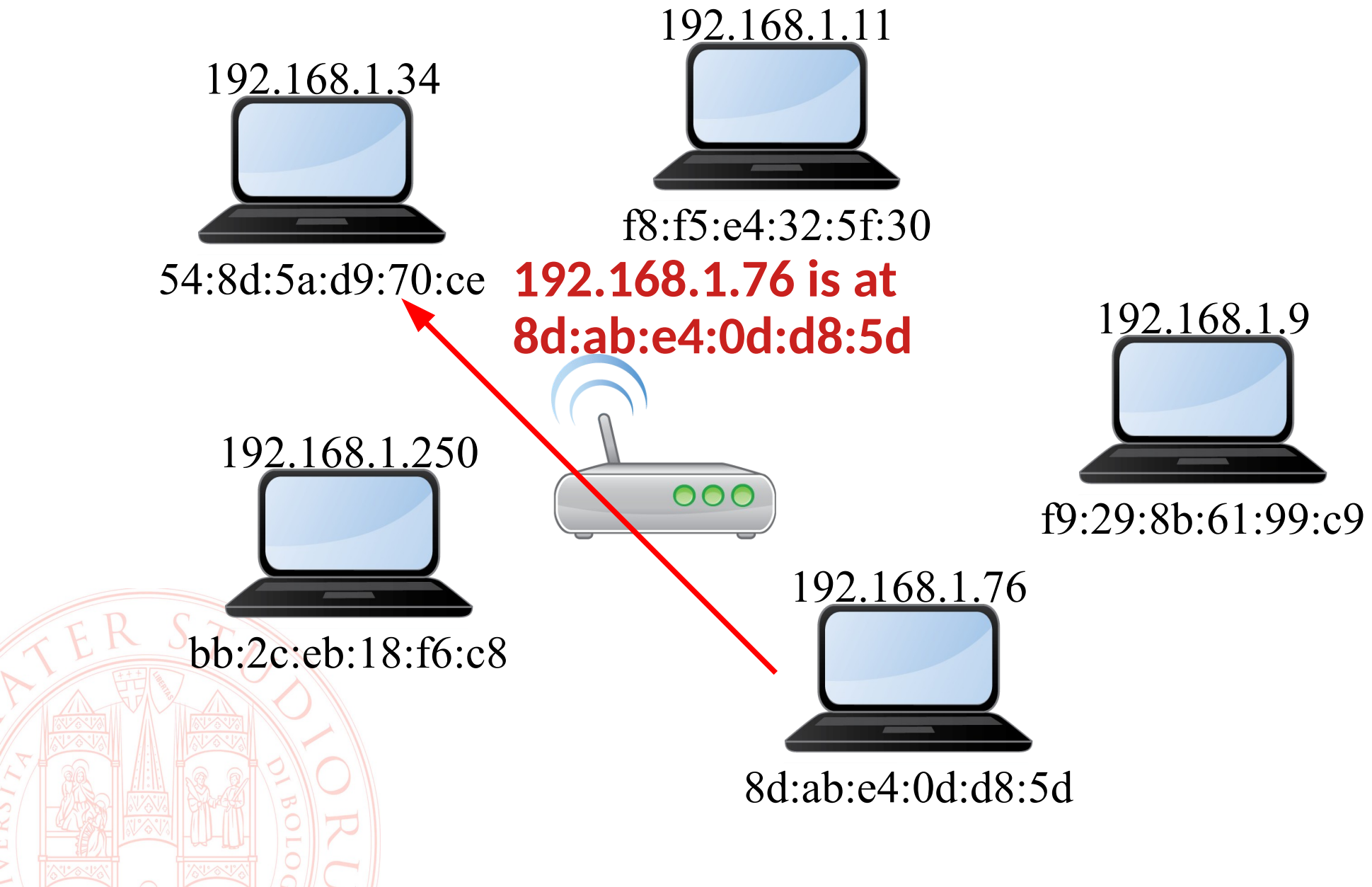
(at 54:8d:5a:d9:70:ce)



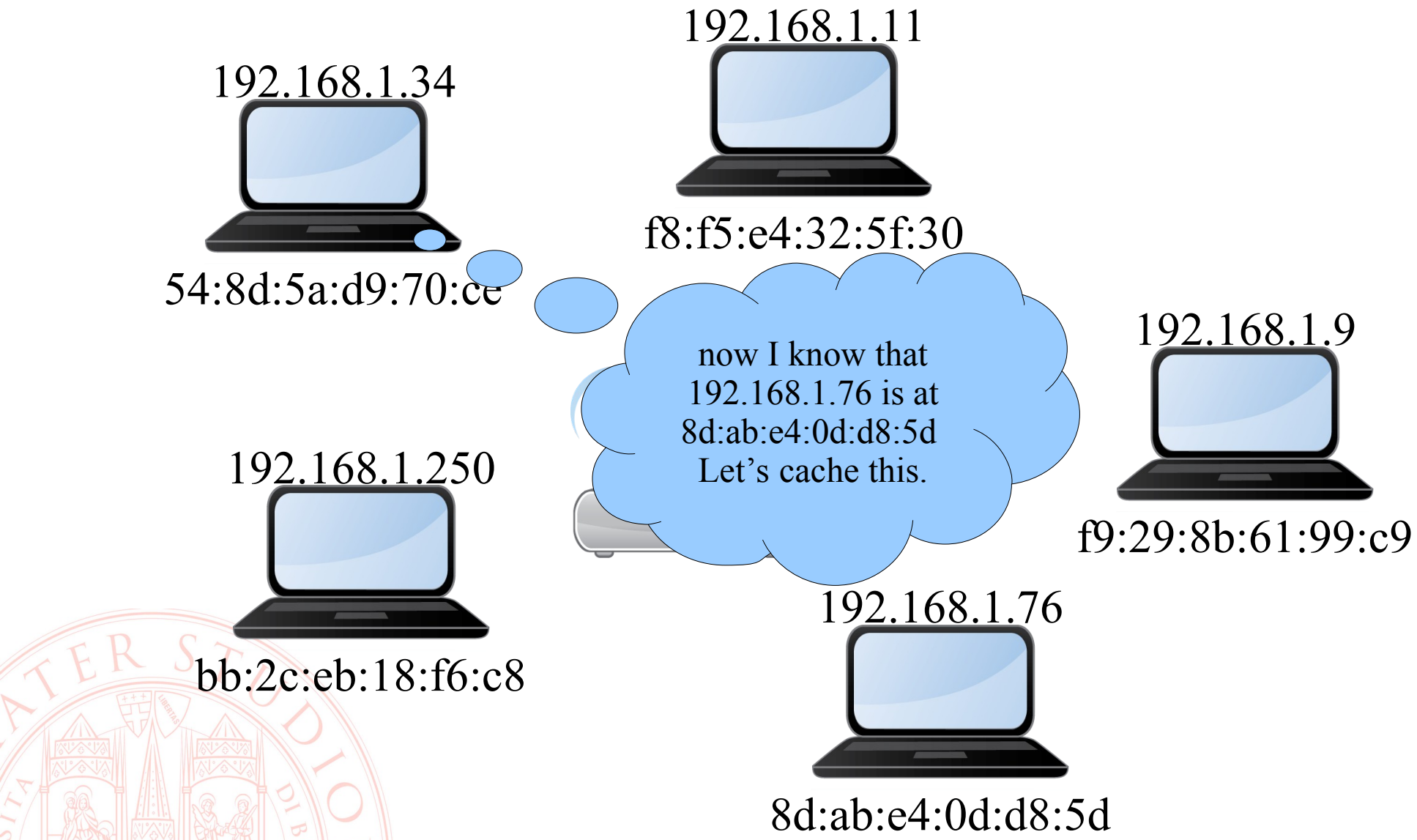
ARP request – caching opportunistico



ARP reply - unicast



ARP reply - unicast



Il livello fisico

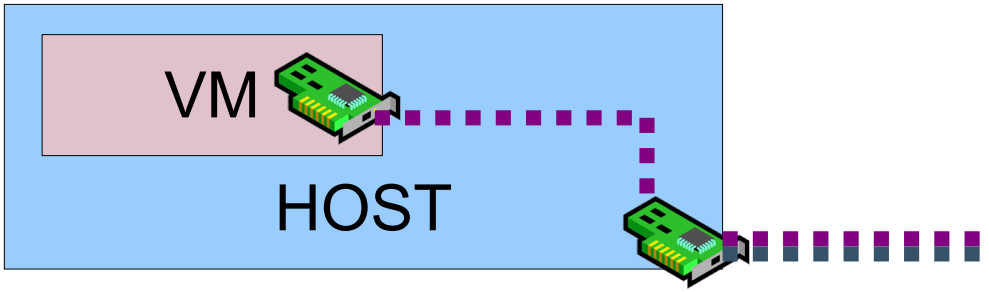
- Sul “ferro”:
  - l’interfaccia di rete è un vero e proprio dispositivo elettronico
  - il MAC address è tipicamente cablato nel dispositivo
  - la sua connessione via cavo oppure la sua associazione a una rete wireless ne definiscono l’appartenenza a una LAN
  - l’indirizzo IP va configurato (vedi seguito)
- In una VM:
  - l’interfaccia di rete è un artefatto gestito dall’hypervisor
  - il sistema operativo guest la percepisce come un dispositivo
  - l’hypervisor
    - può impostare il MAC address
    - definisce a quale segmento di rete è connessa
    - può gestire a volte l’indirizzamento logico e modalità particolari di consegna del traffico

Il livello fisico in VirtualBox

- VirtualBox permette di attivare molteplici interfacce per ogni VM
- Ogni interfaccia può essere connessa in una modalità specifica; quelle principali sono
  - NAT
  - Bridged
  - Host-only
  - Internal
- A default, è attiva una sola interfaccia in modalità NAT
  - permette di navigare attraverso l'host
  - vedremo meglio cosa significa dopo aver introdotto i concetti di instradamento

Il livello fisico in VirtualBox e Vagrant

- Interfacce *bridged*
  - si comportano come se fossero connesse all'interfaccia dell'host attraverso un bridge/hub, quindi è come se fossero attestate sulla stessa LAN dell'host



  - Vagrant può assegnare un'interfaccia bridged a una VM con la direttiva di configurazione

```
config.vm.network "public_network"
```

    - di default assegna automaticamente tutti i parametri
    - è possibile specificare un IP statico che verrà dato alla VM in fase di provisioning

```
config.vm.network "public_network", ip: "192.168.0.17"
```

    - nel caso l'host abbia più interfacce, si può selezionare a quale agganciarsi

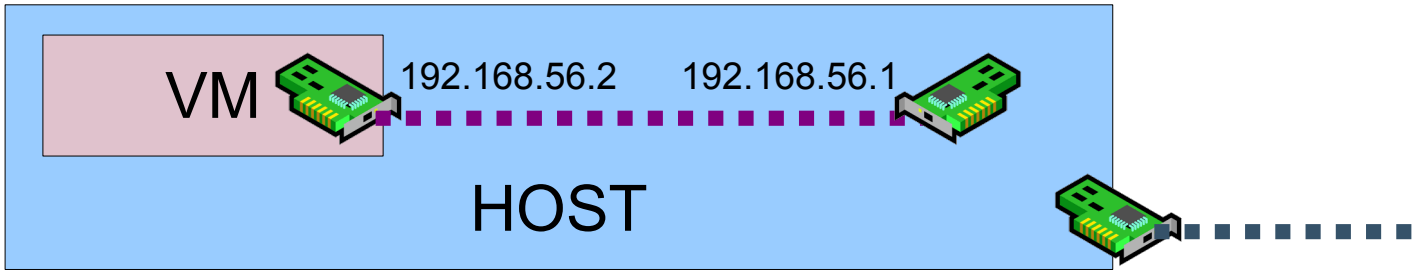
```
config.vm.network "public_network", bridge: "eth0"
```

    - è possibile disabilitare l'automatismo per lasciare che il guest si occupi della configurazione

```
config.vm.network "public_network", auto_config: false
```

Il livello fisico in VirtualBox e Vagrant

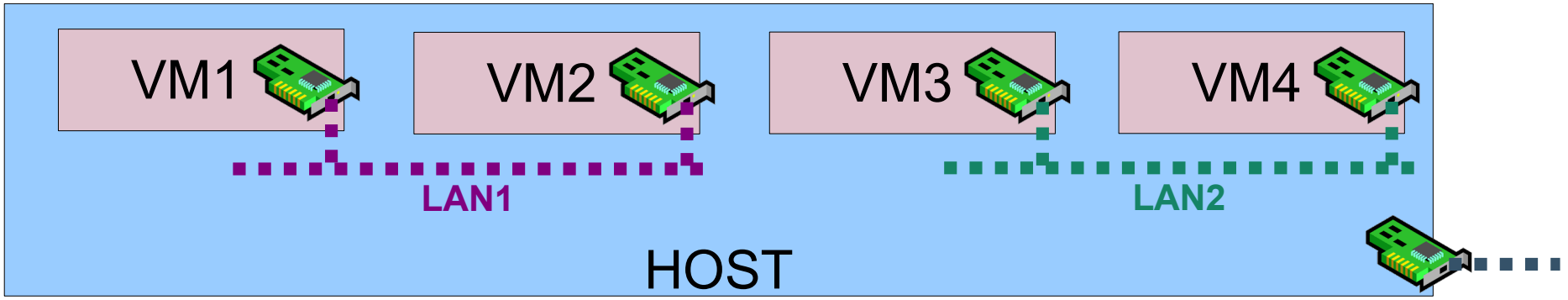
- Interfacce *host-only*
  - l'hypervisor
    - viene configurato per utilizzare una specifica subnet IP
    - genera un'interfaccia virtuale sull'host e le assegna un IP della subnet
    - connette l'interfaccia della VM alla corrispondente LAN virtuale in modo che la VM possa comunicare unicamente con l'host



  - Vagrant può assegnare un'interfaccia host-only a una VM con la direttiva di configurazione `config.vm.network "private_network"`
    - è possibile creare più reti host-only distinte specificandone il nome `config.vm.network "private_network", name: "vboxnet3"`
    - valgono le opzioni `ip` e `auto_config`

Il livello fisico in VirtualBox e Vagrant

- Interfacce *internal*
  - l'hypervisor le assegna a una LAN totalmente virtuale, e fa in modo che solo le interfacce appartenenti alla stessa internal network possano comunicare tra loro

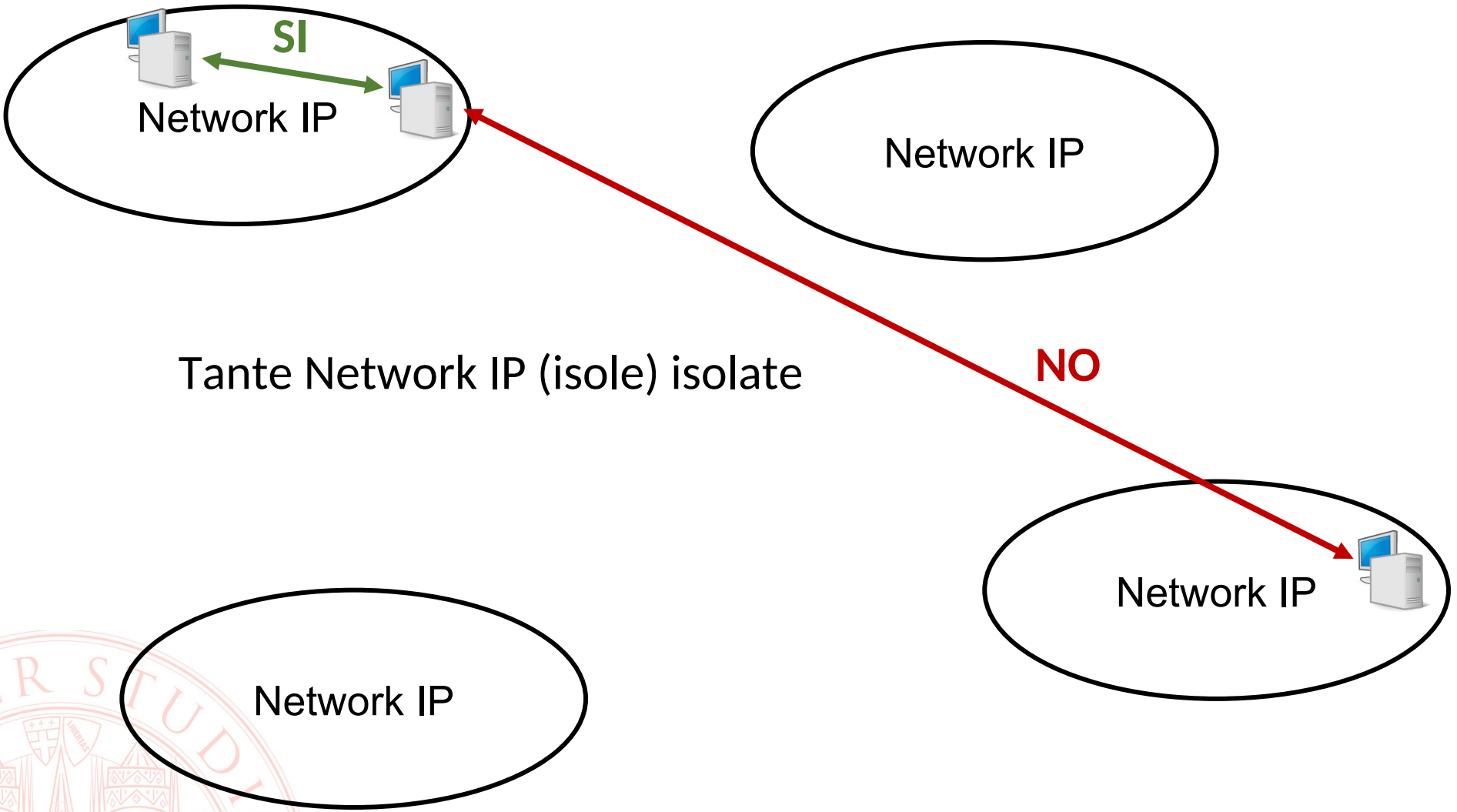


  - Vagrant tratta le interfacce internal come un caso speciale di private_network

```
config.vm.network "private_network", virtualbox__intnet: "LAN1"
```

    - valgono le opzioni `ip` e `auto_config`

Internet: reti di reti



Interconnettere le isole

- Per far parlare tra loro le isole (network IP) è necessario che
  - Vi siano dei collegamenti fra le isole stesse, spesso realizzati con tecnologie diverse da quelle dell'isola
  - Vi siano degli apparati che permettono di usare questi collegamenti nel modo opportuno
  - Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere

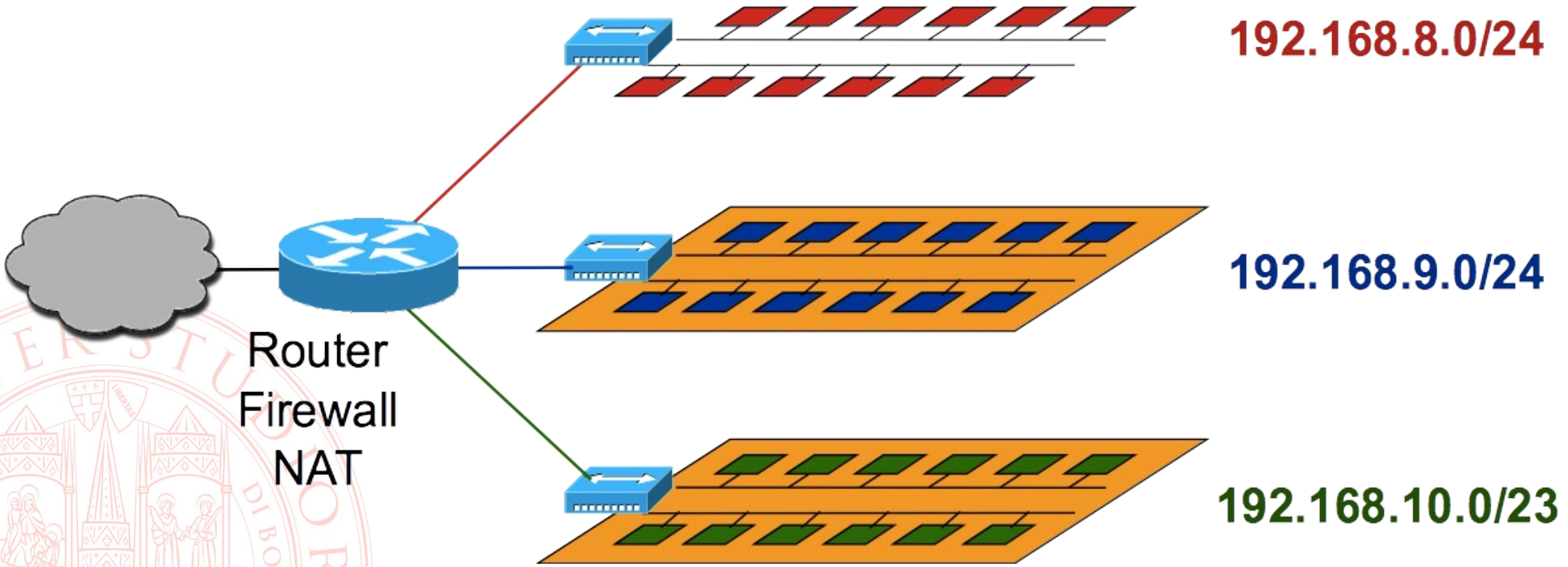
Cosa fa IP

- La tecnologia IP è agnostica rispetto alla tecnologia con cui sono realizzate le network
  - Il protocollo IP è concepito per lavorare indifferentemente su tecnologie diverse

- L'obiettivo di IP è quello di rendere possibile il dialogo fra network a prescindere dalla loro implementazione e localizzazione

Interconnessione di LAN tramite router

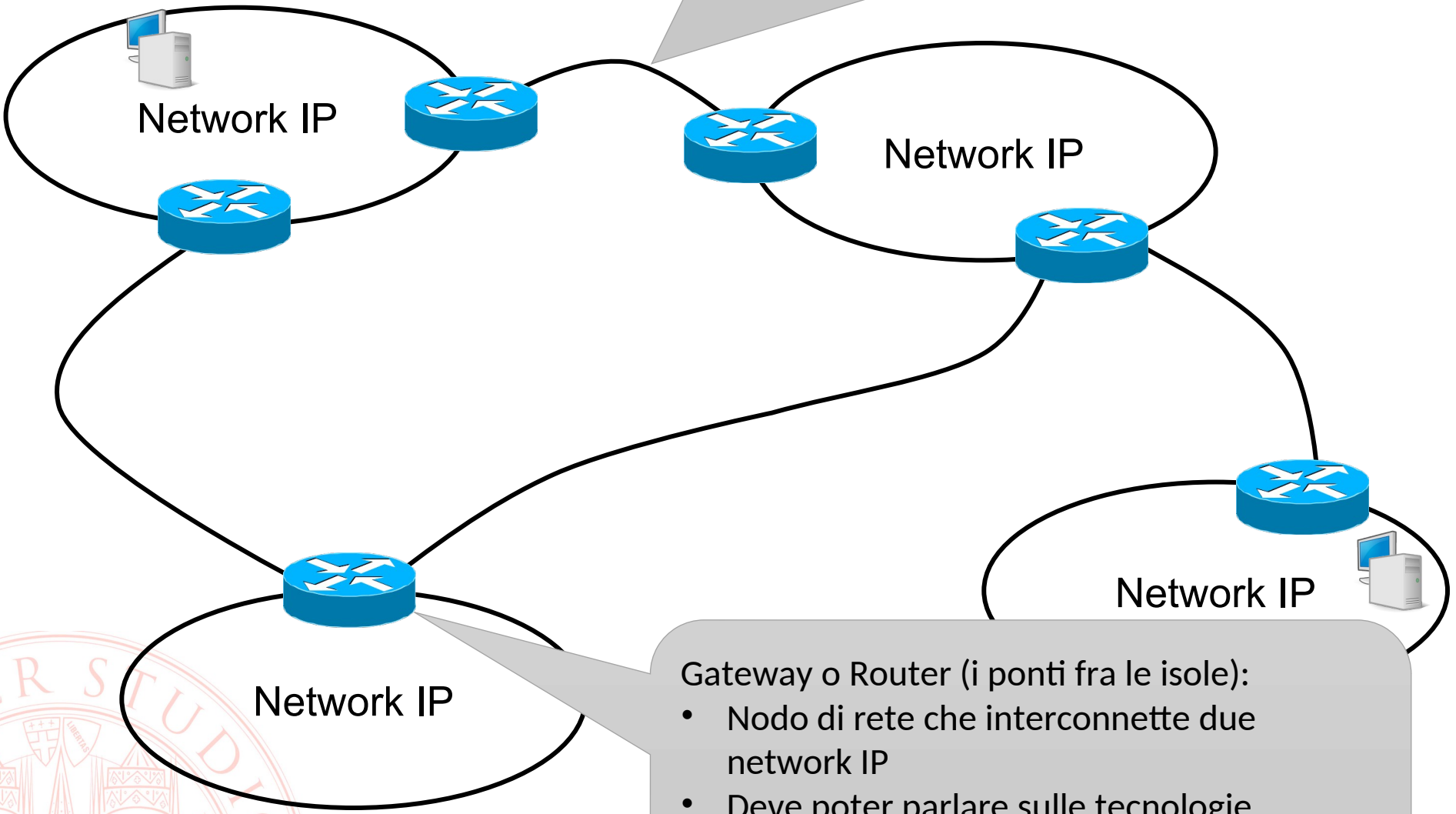
- Domini broadcast separati
- Permette la separazione delle LAN per motivi di
  - efficienza
  - sicurezza
- Limitata mobilità degli host da una LAN all'altra



I router

Collegamento fra router:

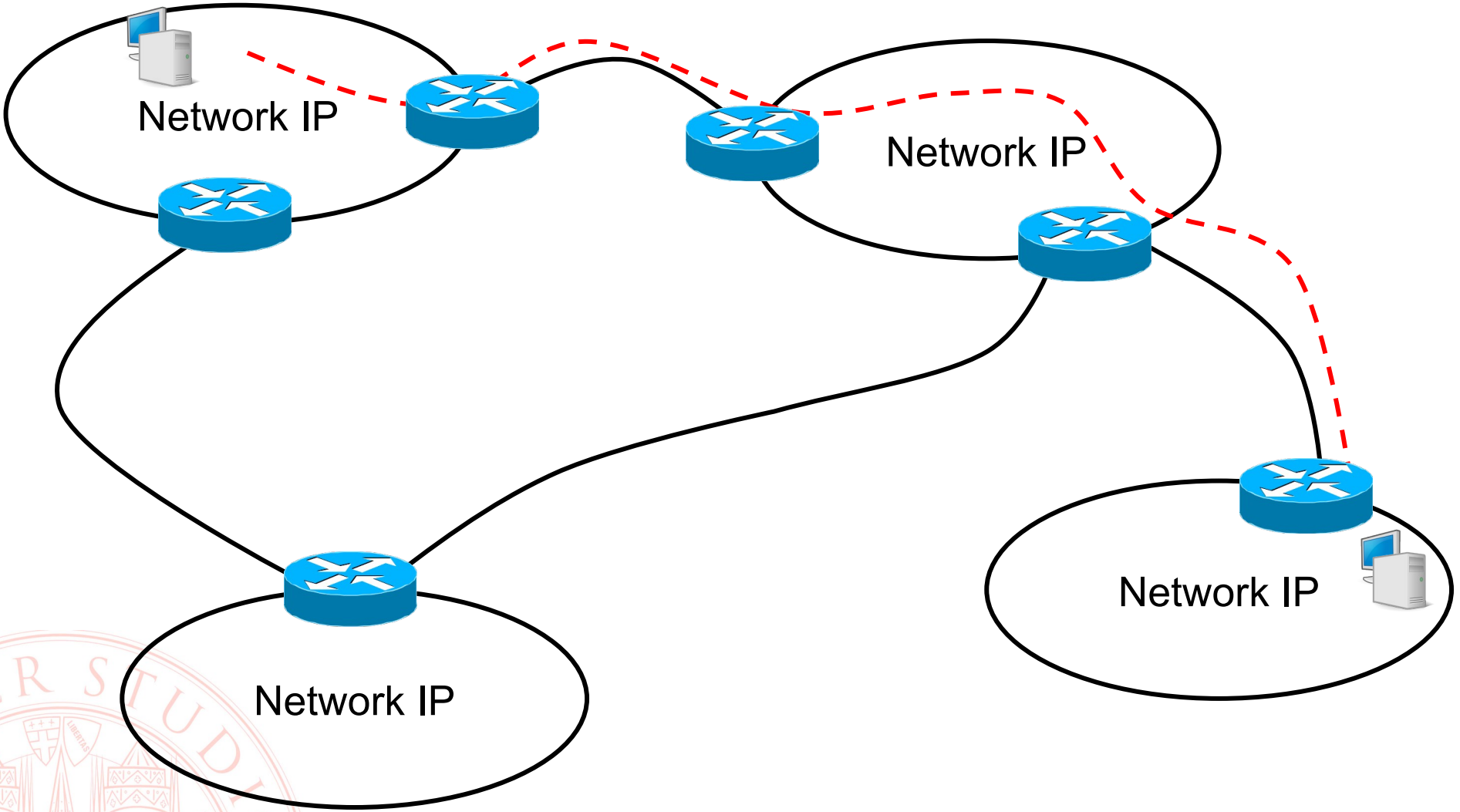
- Può essere una tecnologia simile a quella delle network oppure molto diversa



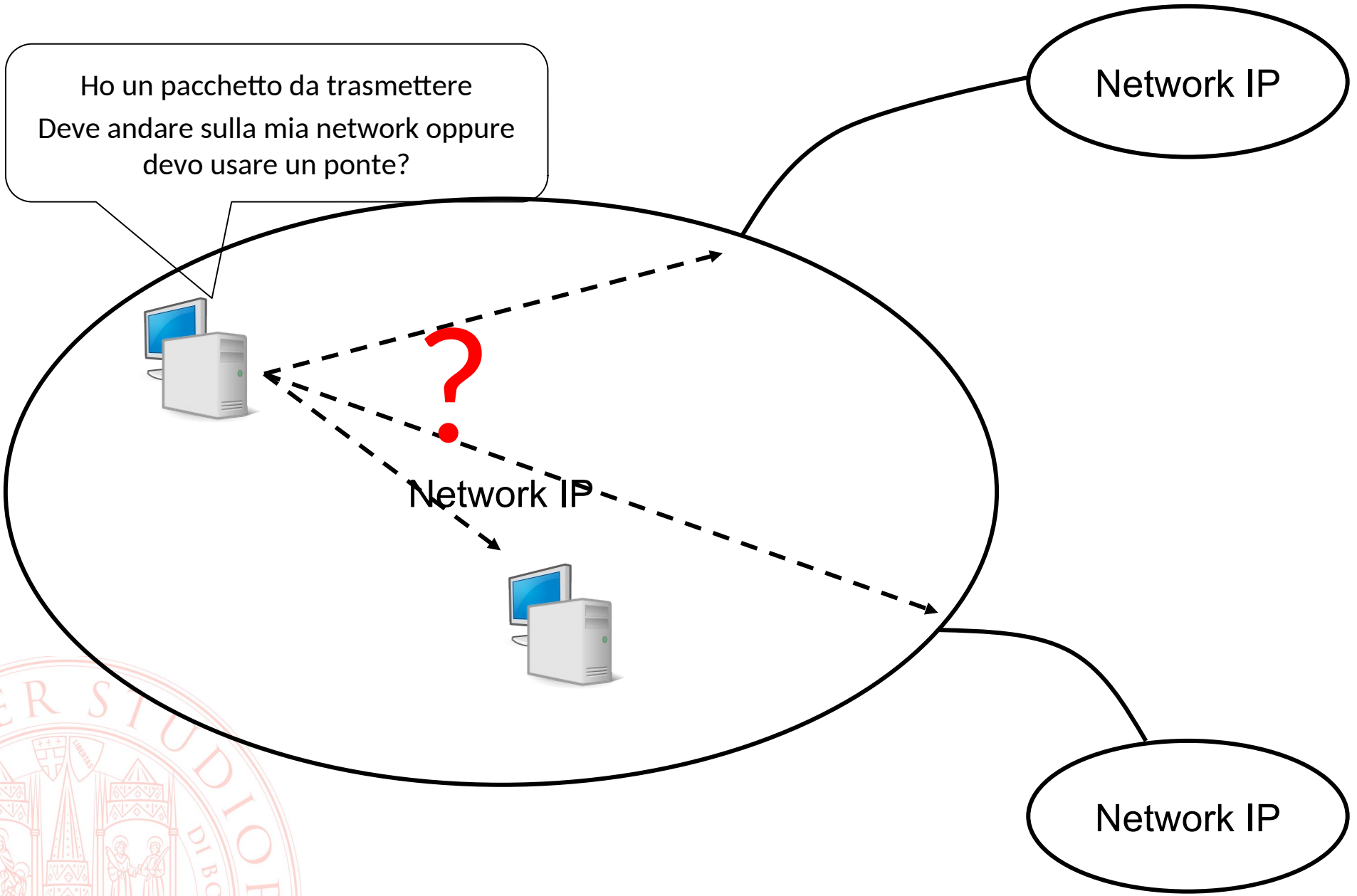
Gateway o Router (i ponti fra le isole):

- Nodo di rete che interconnette due network IP
- Deve poter parlare sulle tecnologie specifiche delle due Network
- Ha funzioni dal livello 1 al livello 3 OSI

Il percorso end-to-end



La domanda cruciale

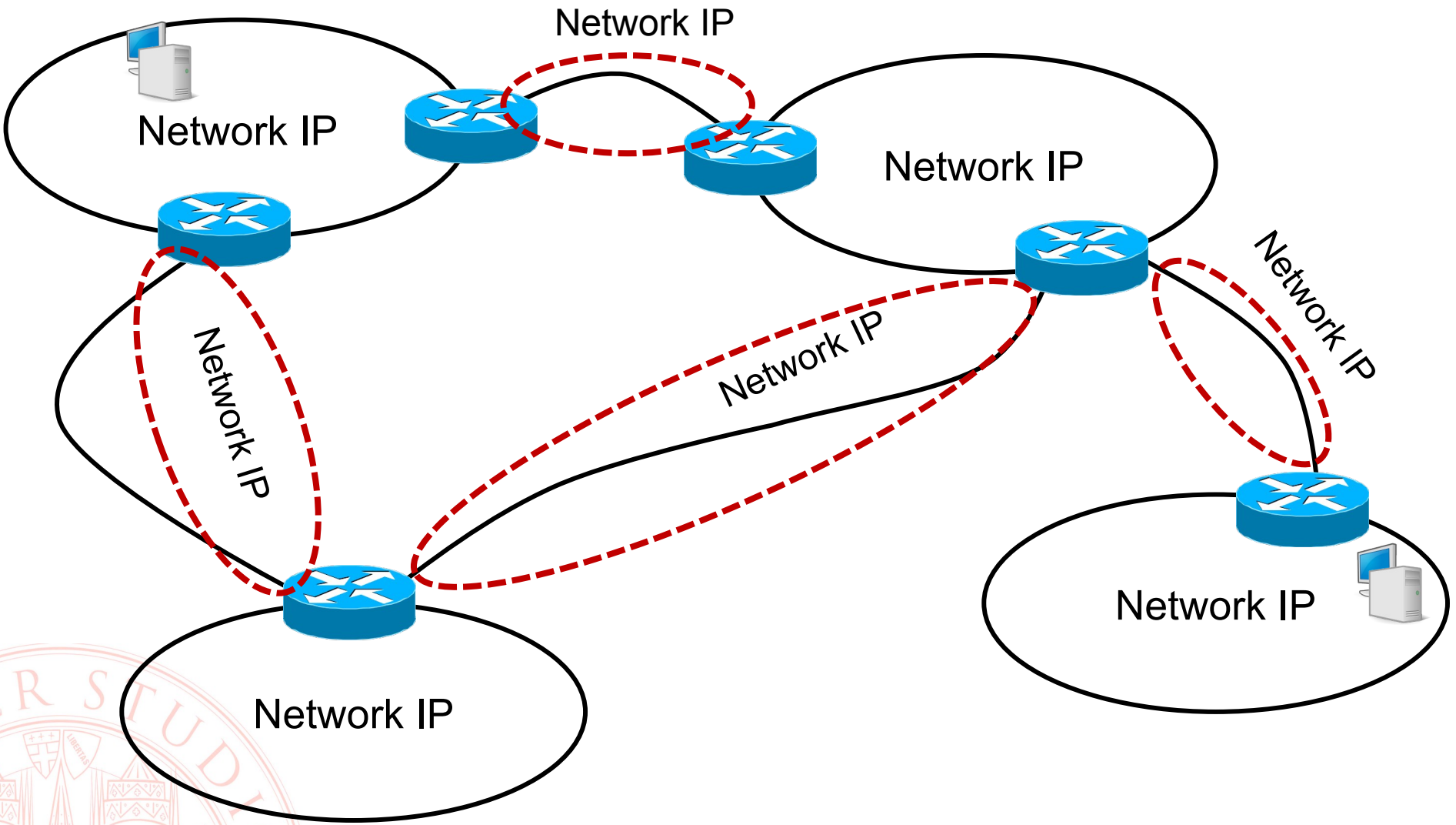


La risposta

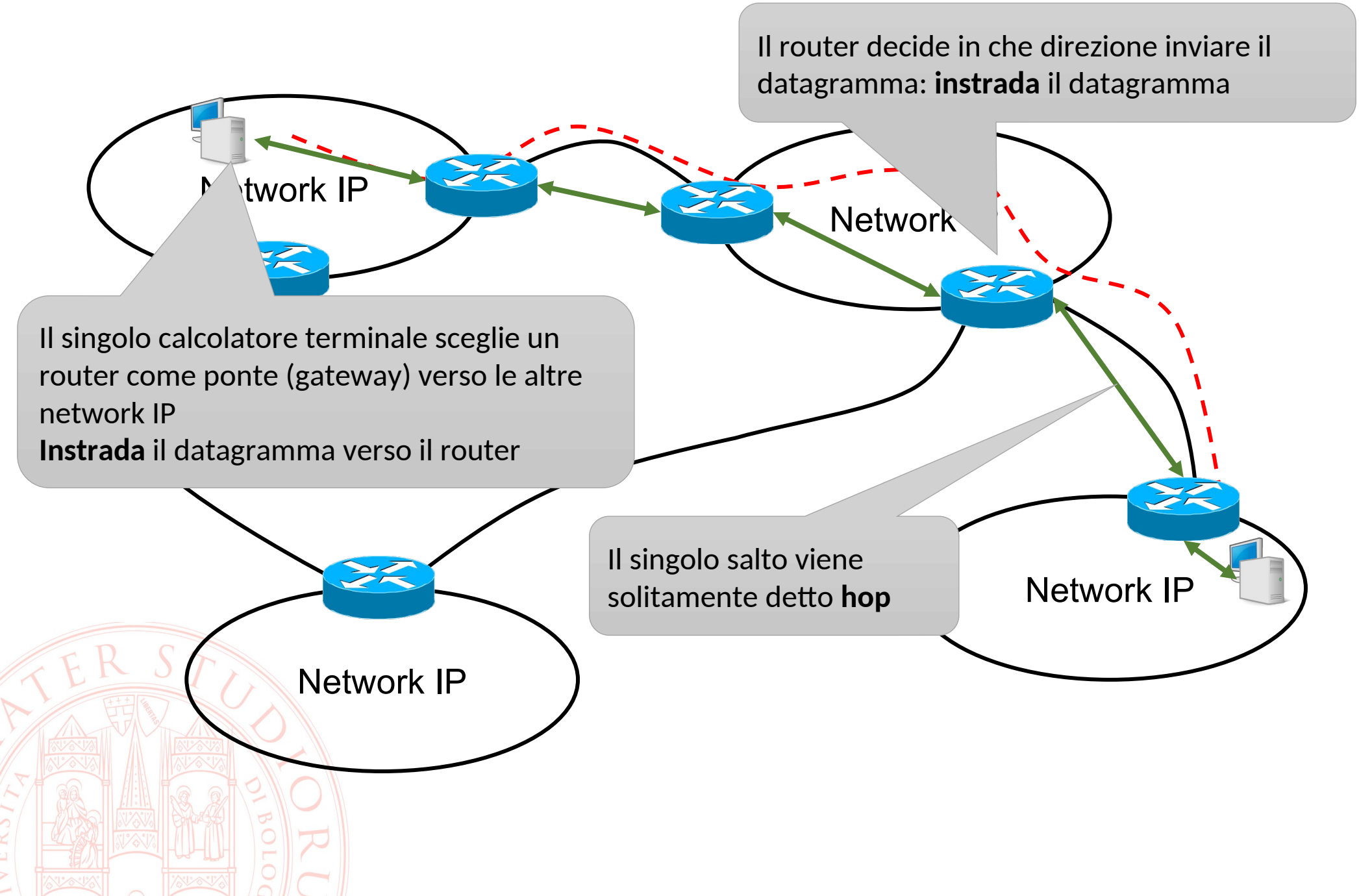
- Ogni nodo di Internet ha una base dati di destinazioni possibili
- Quando deve inviare un datagramma
  - Osserva dall'indirizzo IP di destinazione
  - Legge la base dati
  - Decide quale azione intraprendere

- La tecnologia della propria network può essere utilizzata:
  - Per raggiungere la destinazione finale
  - Per raggiungere il primo ponte da attraversare

Le network fra i router



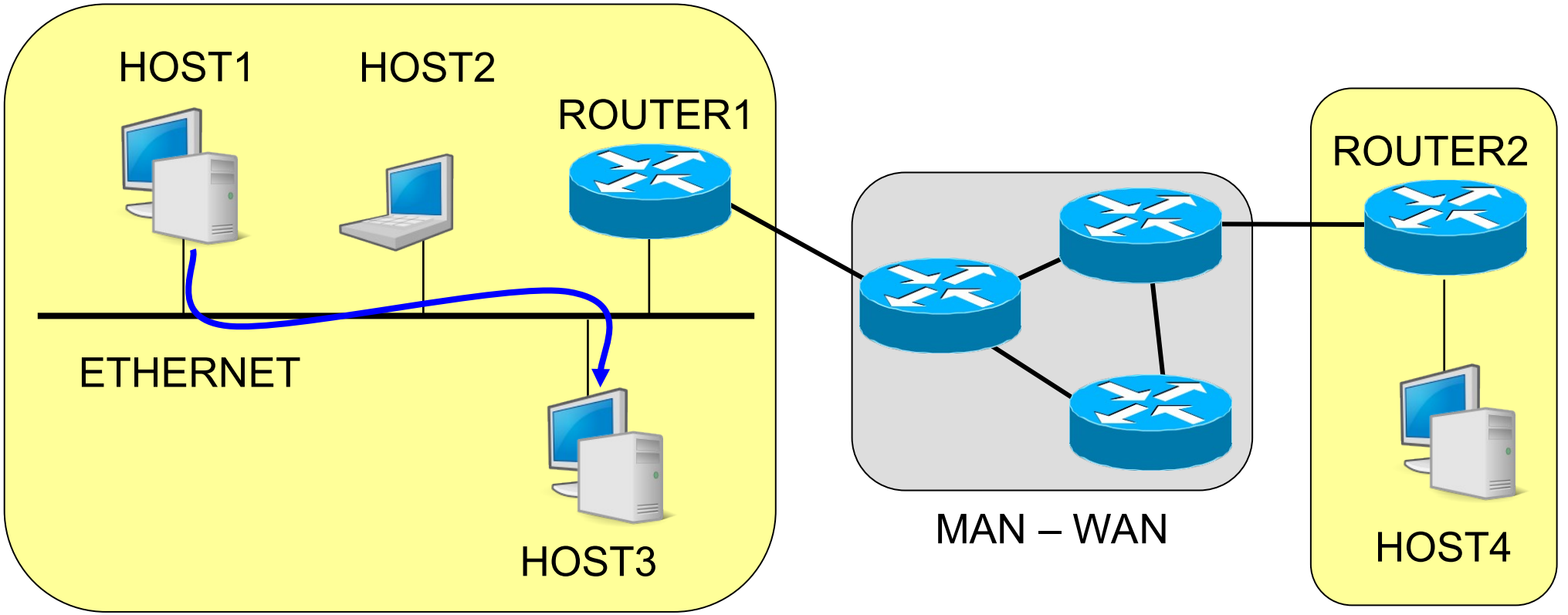
L'instradamento IP



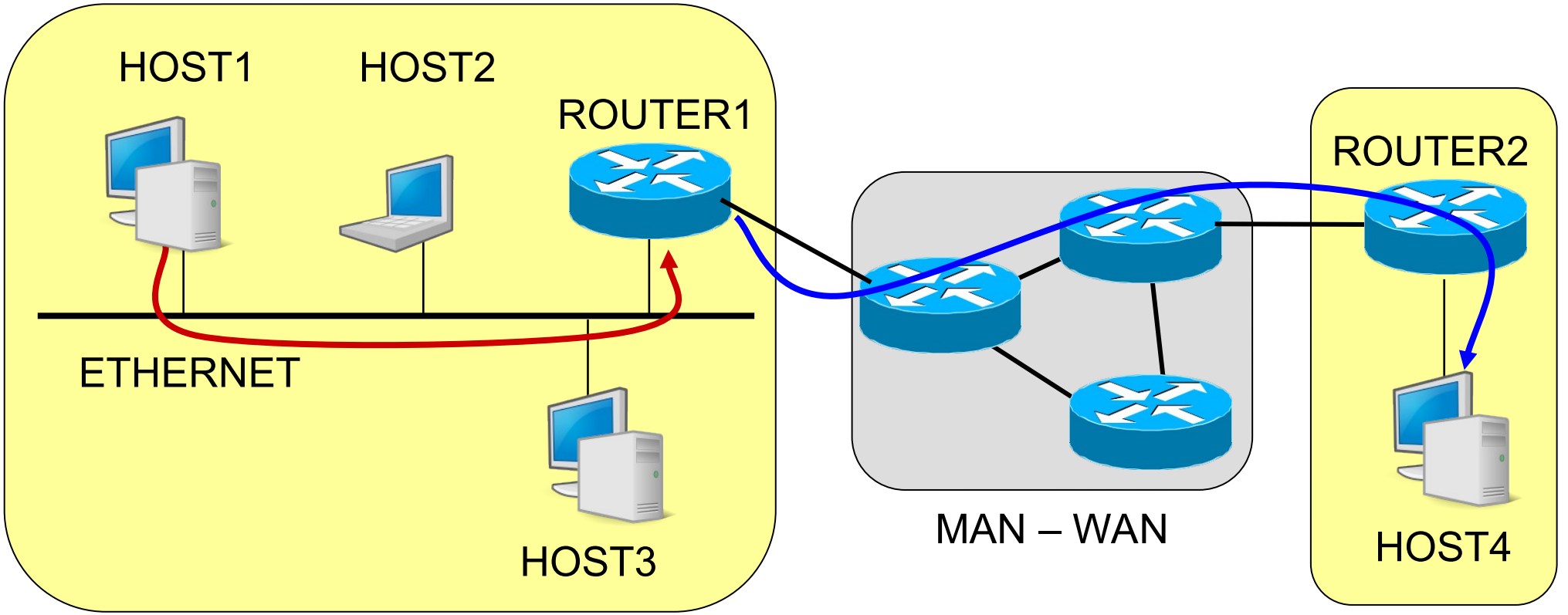
Instradamento diretto e indiretto

- **Routing** : scelta del percorso su cui inviare i dati
  - i router formano struttura interconnessa e cooperante:
    - i datagrammi passano dall'uno all'altro finché raggiungono quello che può consegnarli direttamente al destinatario
- **Direct delivery** :
  - IP sorgente e IP destinatario sono sulla stessa rete fisica
  - L'host sorgente spedisce il datagramma direttamente al destinatario
- **Indirect delivery** :
  - IP sorgente e IP destinatario non sono sulla stessa rete fisica
  - L'host sorgente invia il datagramma ad un router intermedio

Direct Delivery

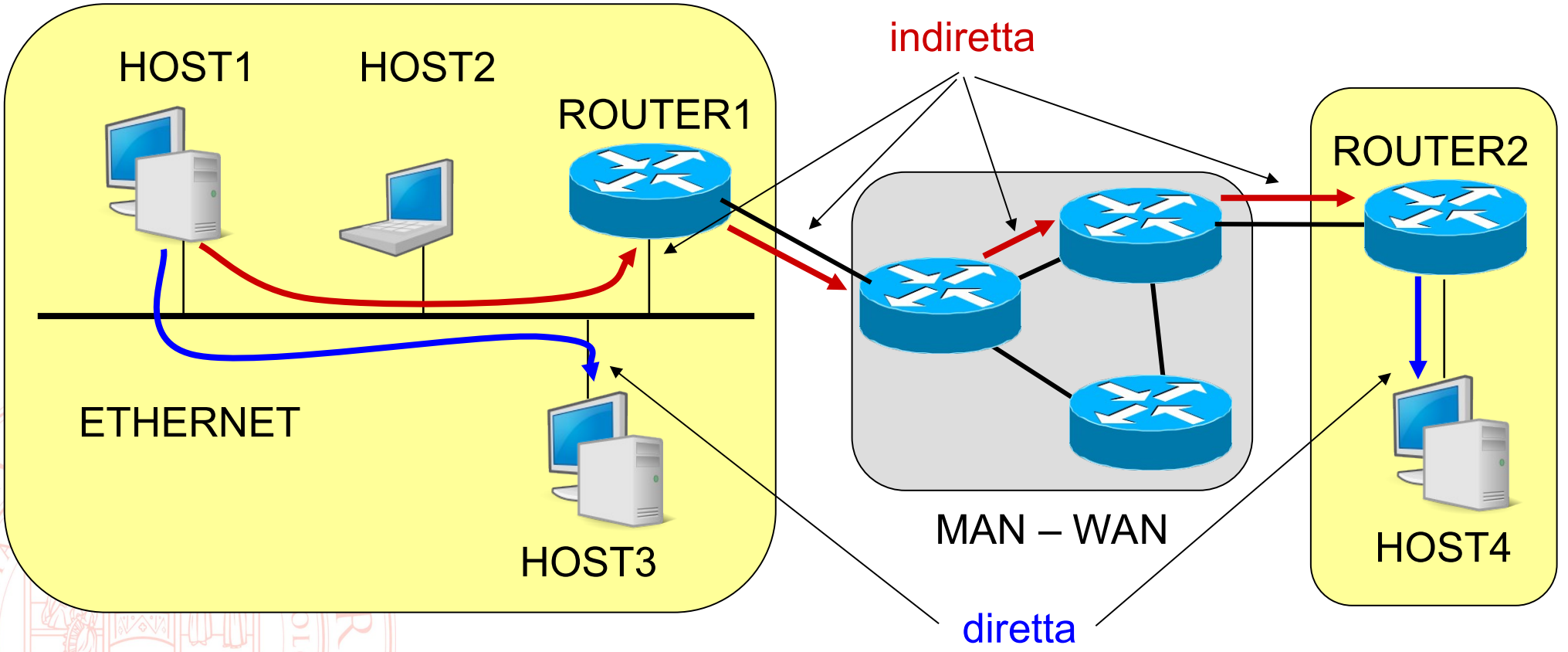


Indirect Delivery



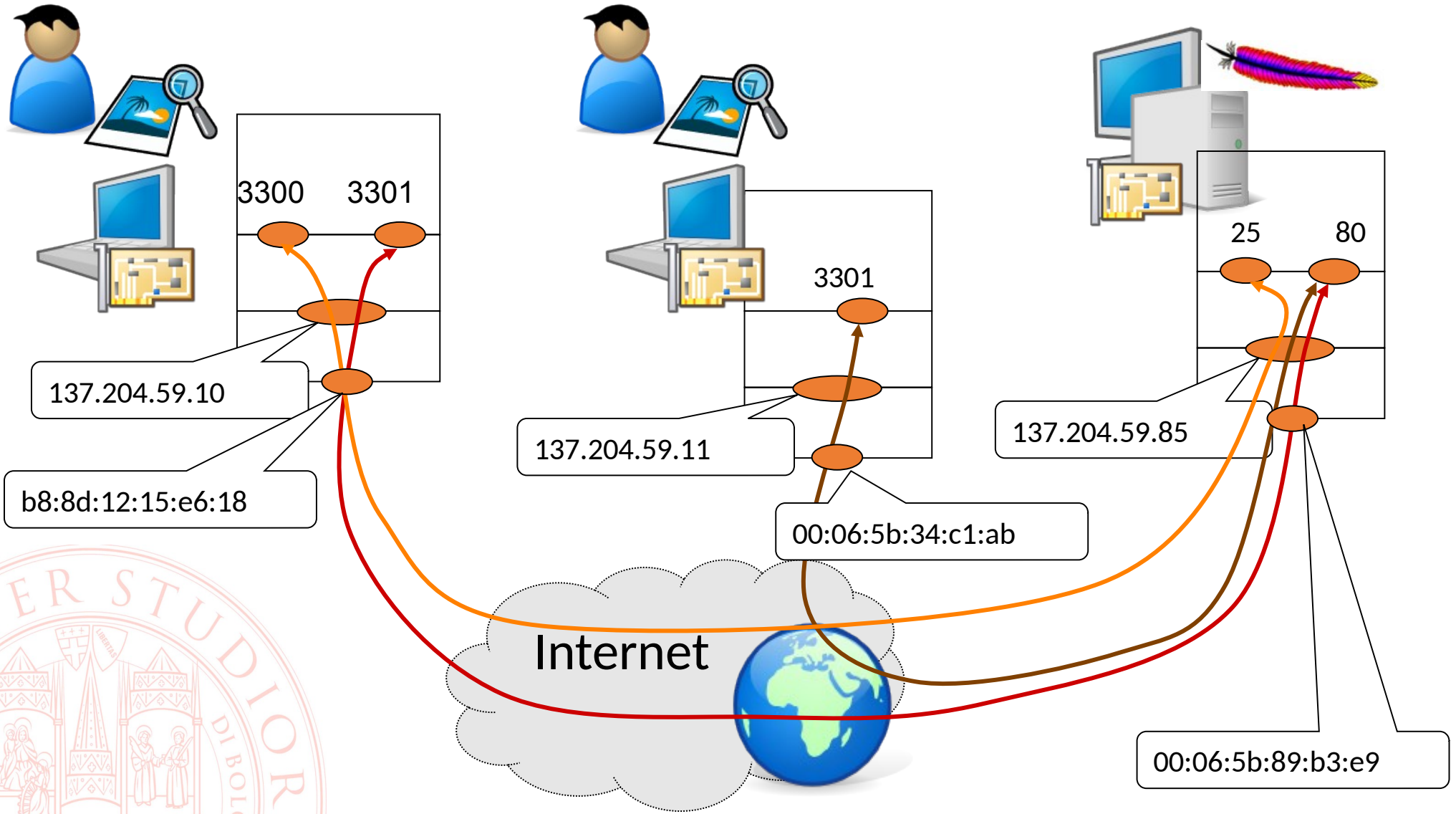
Da mittente a destinatario

- C’è sempre una consegna diretta
- Può non esserci alcuna consegna indiretta
- Possono esserci una o più consegne indirette



Flussi di comunicazione

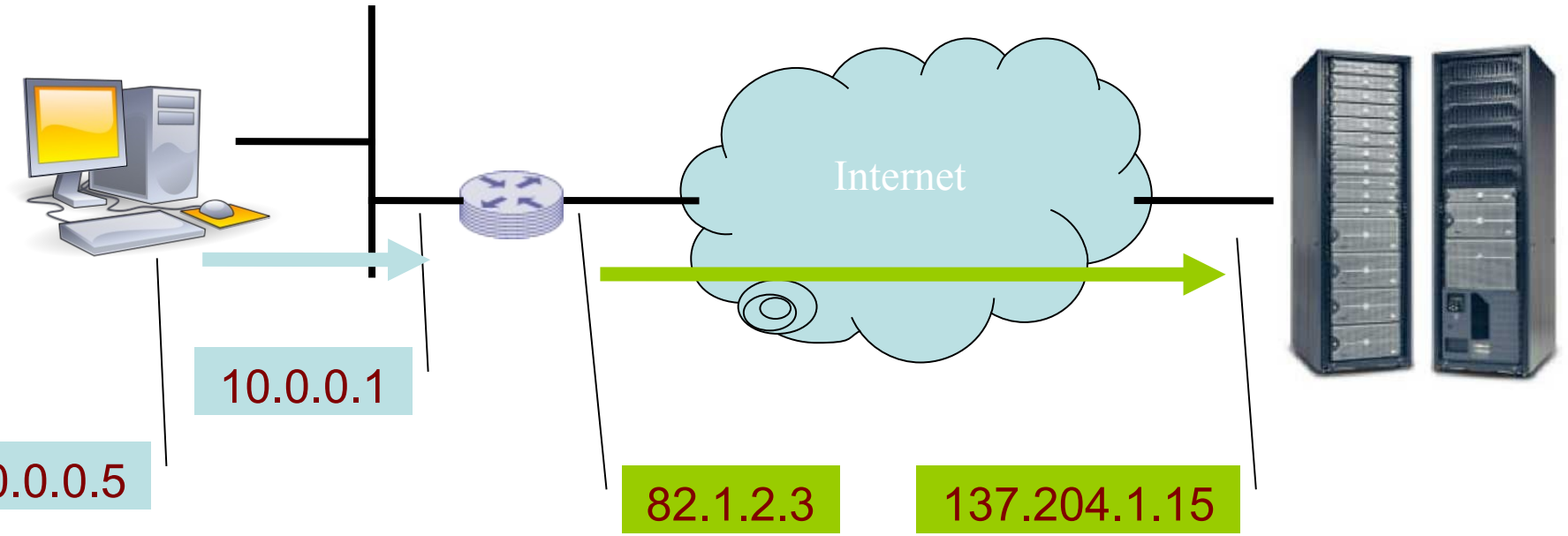
- Infine, il livello di trasporto aggiunge un ulteriore indirizzamento (le porte) per discriminare tra applicazioni in esecuzione sullo stesso host



Network Address Translation (NAT)

- La prospettiva di un esaurimento degli IP disponibili ha fatto esplodere l'utilizzo di una tecnica che consente di utilizzare un solo indirizzo pubblico, senza rinunciare alla possibilità di realizzare in tecnologia TCP/IP una rete anche di grandi dimensioni e di connetterla ad Internet.
- L'efficacia della tecnica si basa sull'osservazione che la gran parte degli host è *client* e non *server*
  - non necessitano di essere raggiunti da richieste
  - originano richieste e devono poter essere raggiunti dalle risposte

Network Address Translation (NAT)



Richiesta

Source	10.0.0.5	: 34567
Destination	137.204.1.15	: 80

Default gateway: 10.0.0.1

Richiesta traslata

Source	82.1.2.3	: 34567
Destination	137.204.1.15	: 80

Network Address Translation (NAT)

- La quintupla
  (protocollo, ip_sorgente, porta_sorgente, ip_destinazione, porta_destinazione)
  identifica univocamente una connessione
- Nel NAT molti IP sorgente vengono sostituiti dall'unico IP pubblico del router
  - possibilità di modificare la porta sorgente per disambiguare le connessioni originate con tutti i parametri identici a parte l'IP sorgente
  - memorizzazione delle traslazioni per poter riconoscere il destinatario delle risposte

Source IP	Source port	Router IP	Router port	Dest. IP	Dest. port
10.0.0.5	11111	82.1.2.3	11111	137.204.1.15	80
10.0.0.9	11111	82.1.2.3	11111	137.204.1.15	80

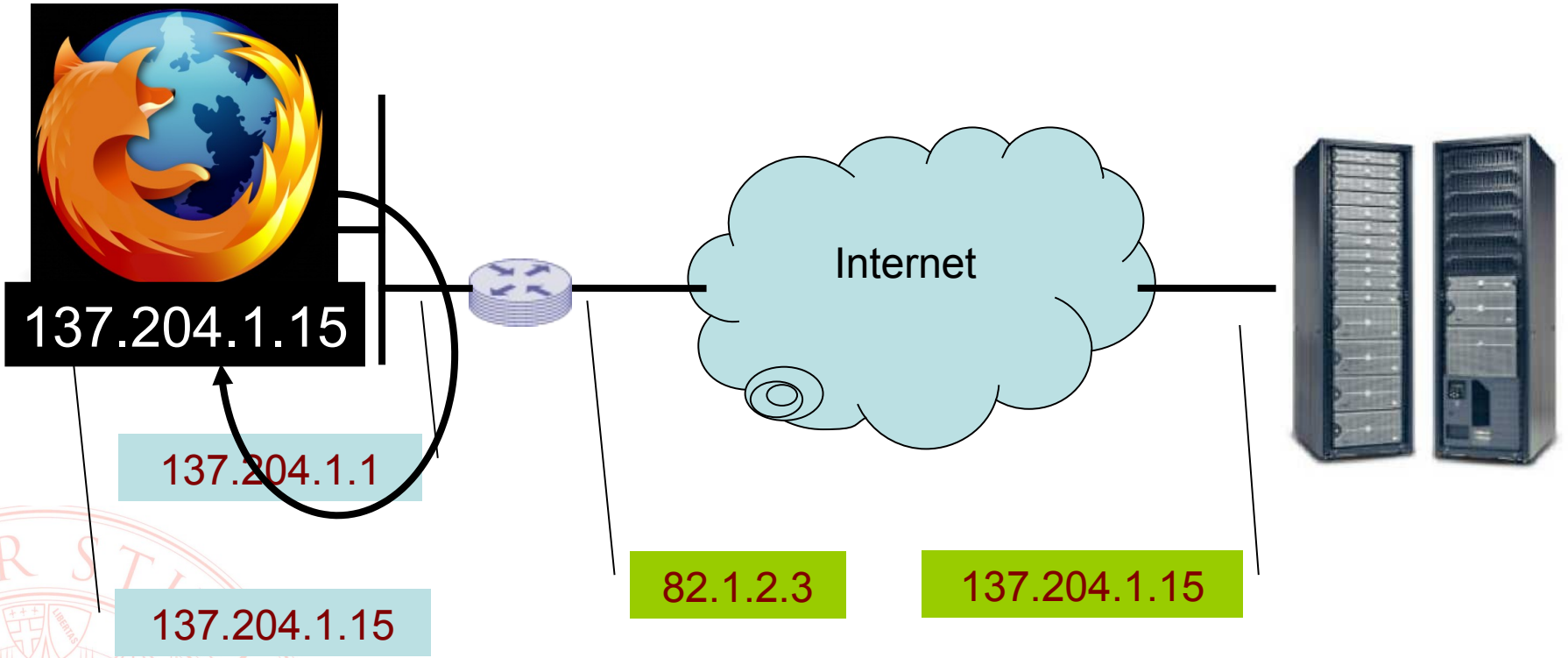
Network Address Translation (NAT)

- La quintupla
  (protocollo, ip_sorgente, porta_sorgente, ip_destinazione, porta_destinazione)
  identifica univocamente una connessione
- Nel NAT molti IP sorgente vengono sostituiti dall'unico IP pubblico del router
  - possibilità di modificare la porta sorgente per disambiguare le connessioni originate con tutti i parametri identici a parte l'IP sorgente
  - memorizzazione delle traslazioni per poter riconoscere il destinatario delle risposte

Source IP	Source port	Router IP	Router port	Dest. IP	Dest. port
10.0.0.5	11111	82.1.2.3	11111	137.204.1.15	80
10.0.0.9	11111	82.1.2.3	22222	137.204.1.15	80

Network Address Translation (NAT)

- Gli IP della rete interna risultano del tutto nascosti
- Cosa capiterebbe scegliendoli arbitrariamente?



IP privati (RFC 1918)

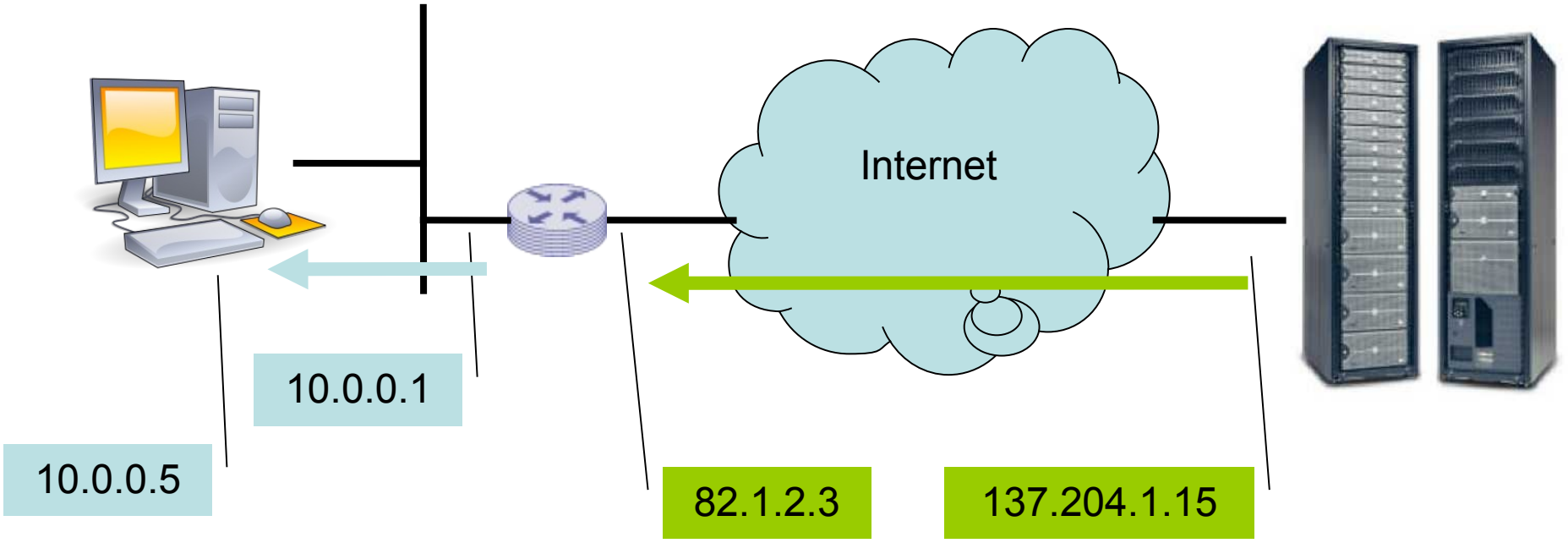
- Per evitare il problema del possibile "oscuramento" di IP validi, uno standard definisce alcuni intervalli di indirizzi che non possono essere utilizzati su Internet
  - `10.0.0.0/8`
  - `172.16.0.0/16  -- 172.31.0.0/16`
  - `192.168.0.0/24 -- 192.168.255.0/24`

SNAT / DNAT

- Per poter utilizzare una rete di client con un solo IP pubblico si modifica l'IP **sorgente**
  - Source NAT (SNAT)
  - il traffico fluisce spontaneamente attraverso il default gateway, che lo maschera: comportamento **trasparente ed automatico**

- Lo stesso dispositivo di instradamento consente anche di rendere raggiungibili dall'esterno alcuni host della rete privata, modificando l'indirizzo di destinazione quando riceve richieste su di una specifica porta del proprio IP pubblico
  - Destination NAT (DNAT)
  - la mappatura tra porta (servizio) di destinazione ed host interno a cui inoltrare la richiesta va **esplicitamente configurata**

DNAT

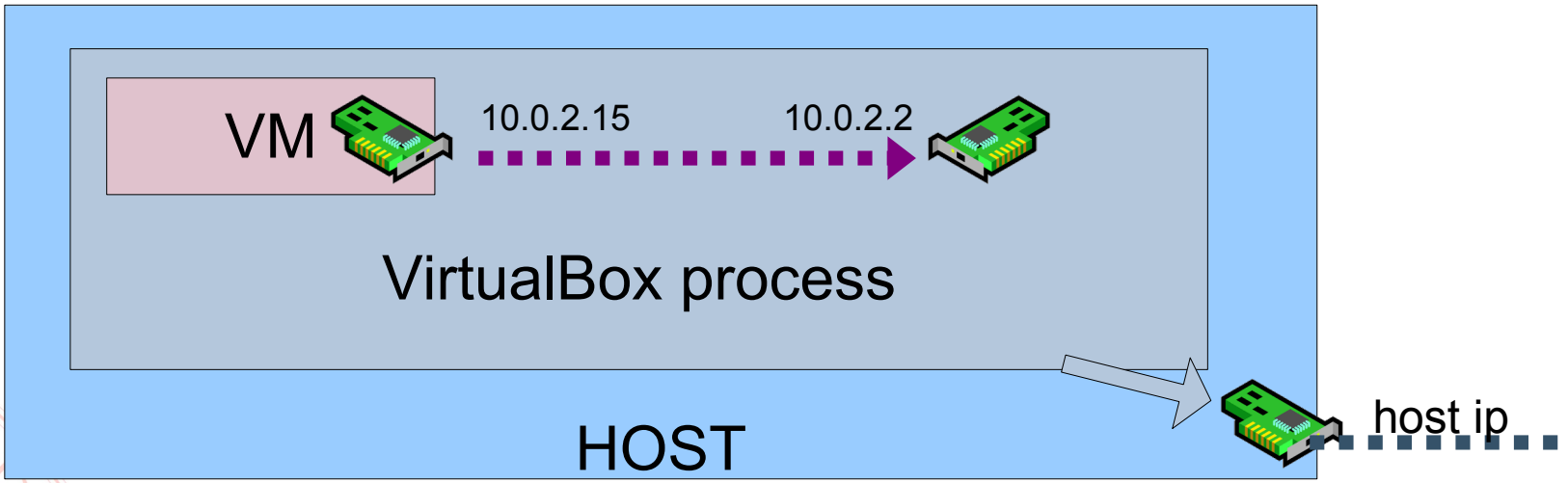


Richiesta traslata	
Source	137.204.1.15 : 34567
Destination	10.0.0.5 : 80

Richiesta	
Source	137.204.1.15 : 34567
Destination	82.1.2.3 : 80

SNAT in VirtualBox e Vagrant

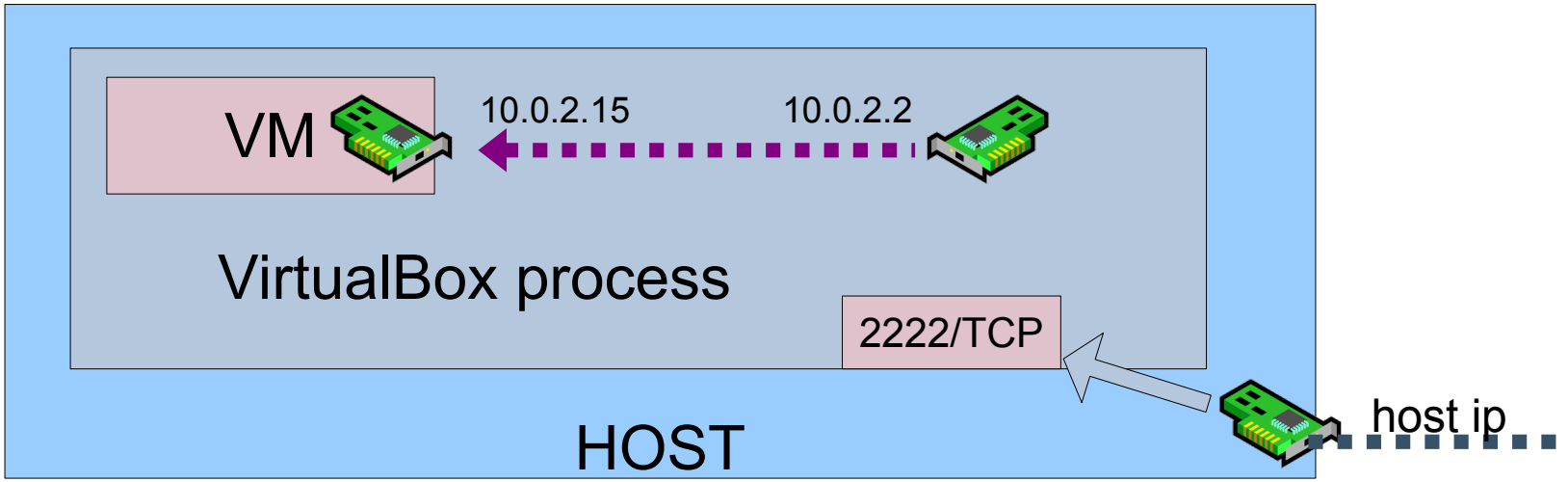
- Come anticipato, le VM VirtualBox (e di conseguenza Vagrant, per noi) nascono con un'interfaccia di tipo NAT
- VirtualBox stesso fa implicitamente da SNAT-Router
  - la VM viene configurata per usare come default gateway una interfaccia virtuale che consegna i pacchetti al processo VirtualBox
  - VirtualBox li propaga all'host OS come se li avesse generati lui stesso, e quindi vengono etichettati con l'IP sorgente dell'host



  - I parametri (IP e MAC) dell'interfaccia sono normalmente assegnati in modo automatico, ma possono essere configurati con `config.vm.base_mac` e `config.vm.base_address`

DNAT in VirtualBox e Vagrant

- È possibile accedere a una VM “NATtata” configurando VirtualBox perchè si comporti anche da DNAT-Router
  - il processo VirtualBox si mette in ascolto su di una porta TCP o UDP dell’host
  - il traffico entrante viene modificato assegnando come destinazione l’IP della scheda virtuale NAT del guest



  - Si possono configurare queste mappature di porte con, ad esempio:
    `config.vm.network "forwarded_port", guest: 80, host: 8080`
  - Il parametro opzionale `host_ip` può essere usato per limitare la raggiungibilità della porta, es. `host_ip: "127.0.0.1"`

Informazioni di sistema

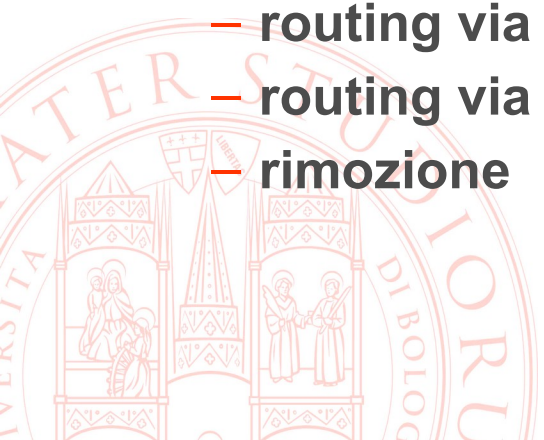
- La configurazione di un'interfaccia di rete richiede come minimo
  - indirizzo IP
  - netmask
- più, se la rete locale è interconnessa ad altre
  - gateway specifici
  - default gateway
- e, se è disponibile un sistema di risoluzione di nomi
  - indirizzi dei server DNS
  - domini di default per costruire i FQDN

Metodi di configurazione

- Le informazioni possono essere assegnate
  - manualmente
  - da un server DHCP
  - localmente in modo automatico
- Attenzione alla dicotomia tipica runtime/persistenza
  - comandi per cambiare istantaneamente la configurazione
  - configurazione da applicare all'avvio
- Attenzione alle interfacce utente di configurazione
  - metodo classico: editing file di testo
    - segue l'approccio standard di qualsiasi servizio
    - modifiche non applicate fino a `systemctl restart networking` (o equivalenti)
  - metodo di default in molte distribuzioni di Linux: **NetworkManager**
    - se presente, può essere pilotato da GUI o `nmcli`
    - può sovrascrivere le modifiche runtime in qualsiasi momento

Configurazione runtime

- suite iproute2
  - comando ip + sottocomandi, sostituisce ifconfig e route
  - controllo completo di tutti gli aspetti più avanzati (link layer, interfacce virtuali, tunnel, VXLAN, policy-based routing, ...)
- sottocomando address (a)
  - visualizzazione `ip a`
  - assegnazione `ip a add <address>/<mask> dev <interface>`
  - rimozione `ip a del <address>/<mask> dev <interface>`
- sottocomando route (r)
  - visualizzazione `ip r`
  - routing via gw `ip r add <dst_net>/<mask> via <gw_addr>`
  - routing via dev `ip r add <dst_net>/<mask> dev <interface>`
  - rimozione `ip a del <address>/<mask>`



Configurazione "classica" Debian

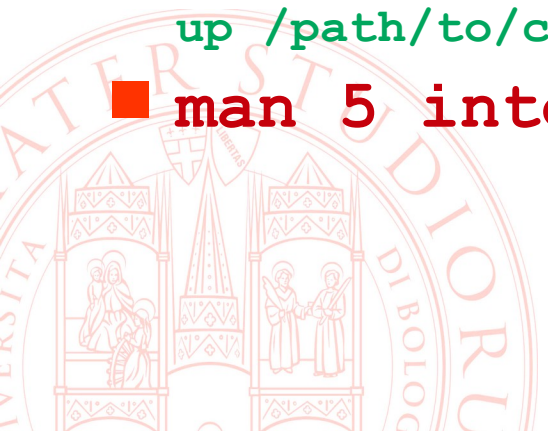
- file `/etc/network/interfaces`
- *snippet* nella cartella `/etc/network/interfaces.d/`
- esempio tipico

```
auto eth0                          # attiva con ifup -a
iface eth0 inet static             # con dhcp al posto di static,
                                   # non serve altro
address 192.168.56.203
netmask 255.255.255.0                 # se omesso, class-based
```

  - opzionalmente

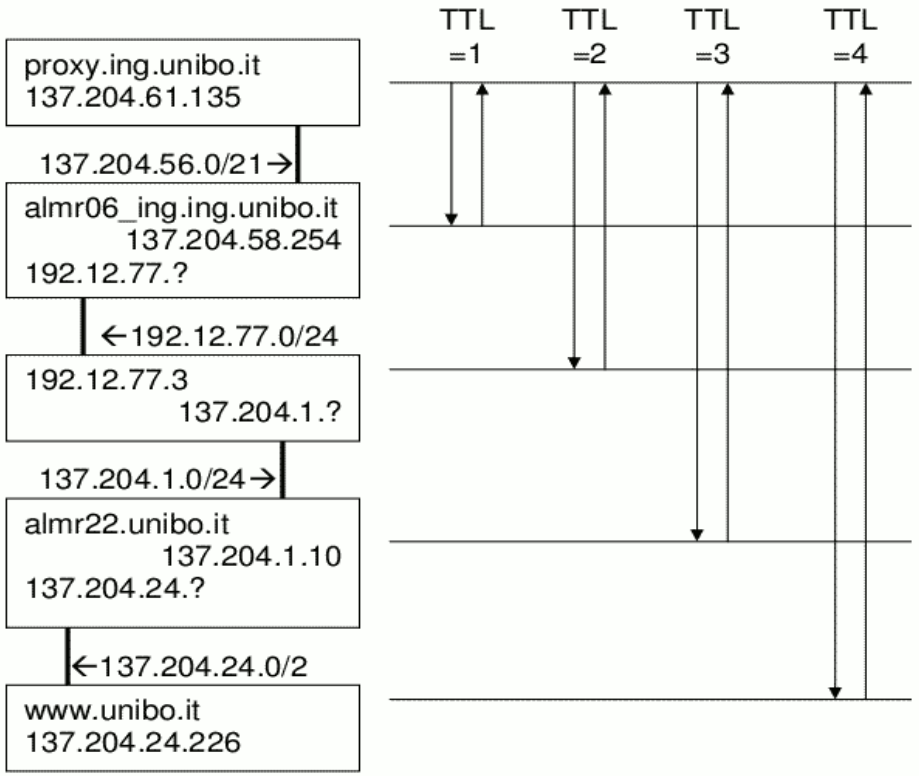
```
gateway 192.168.56.1               # uno solo, non per interfaccia
up /path/to/command arguments      # eseguito dopo configurazione
```

- `man 5 interfaces`



Tool di monitoraggio

- Verifica di base della connettività
  - `ping <IP>`
- Verifica del percorso dei pacchetti
  - `traceroute <IP>`




```
[proxy@proxy proxy]$
     /usr/sbin/traceroute www.unibo.it

traceroute      to      cesias.alma.unibo.it
(137.204.24.226),  30  hops  max,  40  byte
packets

 1  almr06_ing (137.204.58.254)  1.578 ms
 2  192.12.77.3 (192.12.77.3)  4.246 ms
 3  almr22.unibo.it (137.204.1.10)  3.504 ms
 4  cesias.alma.unibo.it (137.204.24.226)
                                  3.108 ms
[proxy@proxy proxy]$
```

Tool di monitoraggio

- Verifica dello stato delle connessioni
  - `ss`
    - `-t / -u` TCP/UDP only
    - `-l / -a` stato LISTEN (il default è ESTABLISHED) / ALL
    - `-n` non risolvere gli indirizzi/porte in nomi simbolici
    - `-p` mostra processi che usano la socket
- Intercettazione del contenuto dei pacchetti
  - `tcpdump`
  - `wireshark`

  → man pages e documentazione